УДК 004.056:061.068

А.В. Сидоренко, К.С. Мулярчик

МОДИФИКАЦИЯ МЕТОДА ШИФРОВАНИЯ ДАННЫХ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

Рассматривается метод шифрования, основанный на использовании tent-отображения и схемы с нелинейным подмешиванием информационного сигнала к хаотическому. Приводится теоретическое обоснование целесообразности применения дискретного (целочисленного) отображения в схеме кодирования при ее практической реализации. Вводятся метод и критерий оценки стойкости рассматриваемого метода к атаке «грубой силой», основанные на изменении выходных характеристик работы метода в зависимости от его начальных параметров. Предлагается модификация метода шифрования, заключающаяся в замене единичного применения хаотического отображения на каждой итерации шифрования последовательностью из n применений и позволяющая улучшить криптостойкость начальной системы. Проводится сравнительный анализ результатов работы схем шифрования с использованием tent-отображения и отображения Чебышева.

Введение

Одним из актуальных направлений в развитом информационном обществе является разработка методов и средств защиты информации, что обусловлено необходимостью обеспечения конфиденциальности передаваемой информации.

В настоящее время в нашей стране и за рубежом ведутся исследования по разработке новых и совершенствованию существующих алгоритмов шифрования [1–4]. Особенно популярной становится разработка криптоалгоритмов, устойчивых к небольшим ошибкам в шифртексте [5–7]. Такие изменения могут быть вызваны помехами в канале связи, сбоями в работе элементов криптоустройств и т. д. При разработке помехоустойчивых криптосистем необходимо учитывать следующее. С одной стороны, криптосистема должна давать на выходе шифртекст с минимальной избыточностью, с другой – для обеспечения помехоустойчивости шифртекст должен обладать избыточностью, достаточной для восстановления ошибочных значений. Совершенные шифры, вообще говоря, должны обладать нулевой избыточностью. Однако в помехоустойчивой криптосистеме при расшифровании информации будет труднее выявить попытки ее модификации.

Теоретический анализ показал, что разработанные алгоритмы шифрования обладают определенными недостатками либо, что встречается гораздо чаще, их криптостойкость к известным и специфическим атакам недостаточно хорошо проанализирована. Поэтому проблемы разработки новых алгоритмов шифрования, совершенствования существующих, а также их глубокого анализа являются весьма актуальными на сегодняшний день.

Развитие теории динамического хаоса в последнее десятилетие способствовало разработке на ее основе новых методов защиты информации. Было установлено, что хаотический сигнал, внешне похожий на шум, может быть потенциально использован в качестве носителя информации, контейнера для передачи полезной информации, скрывая при этом сам факт ее передачи [8, 9].

К настоящему времени выполнен ряд исследований по разработке стойких систем шифрования на основе динамического хаоса. Сформулированы критерии, которым должен удовлетворять криптографически стойкий алгоритм шифрования: после преобразования исходного сообщения в зашифрованном сообщении не должны проявляться какие-либо структуры; схема кодирования должна быть чувствительной по отношению как к открытому тексту, так и ключу шифрования; схема кодирования должна быть симметричной относительно времени кодирования/декодирования; объемы зашифрованного и исходного сообщений не должны сильно отличаться; должна иметься возможность адаптации схемы кодирования к различным видам информационных сигналов и возможность изменения длины ключа, также схема должна быть устойчивой к основным видам криптоатак (атаке методом грубой силы, атаке на основе известного открытого текста и др.) [10–12].

При рассмотрении системы на основе динамического хаоса для криптографических применений было отмечено, что такие свойства, как чувствительность к начальным условиям, асимптотическая независимость начального и конечного состояний, возможность самосинхронизации передатчика и приемника, с одной стороны, присущи динамическому хаосу, а с другой – являются характерными для криптографических алгоритмов [13].

Большинство предлагаемых в литературе методик производят криптографически слабые и медленные алгоритмы. Одна из причин такого положения заключается в необоснованном выборе хаотического отображения для схемы шифрования. Дело в том, что при построении алгоритма шифрования необходимо соблюдать два основных принципа: чувствительности к открытому тексту и чувствительности к ключу [14, 15]. Малейшие изменения в одном из них должны значительно изменять результаты шифрования. В хаотических алгоритмах шифрования роль открытого текста могут играть начальные условия, а роль ключа – параметры отображения. Это означает, что если необходимо использовать в качестве основного элемента схемы некоторое хаотическое отображение, то оно должно обладать чувствительностью не только к начальным условиям, но и к любым возмущениям в пространстве параметров [16]. Известно, что большинство хаотических аттракторов структурно неустойчиво по отношению к изменению параметров. Алгоритмы на их основе могут иметь слабые ключи. Поэтому необходимо осторожно и обоснованно выбирать тип хаотических отображений. Так, например, устойчивый хаос не может встречаться в гладких системах. С другой стороны, структурно устойчивый хаос может наблюдаться в кусочно-линейных отображениях.

1. Система шифрования на основе динамического хаоса

Анализ систем криптографической защиты информации показывает, что они состоят из определенного числа логических элементов (блоков). Схему такой системы можно приблизительно описать следующим образом: «источник информации – блок зашифрования – канал передачи данных – блок расшифрования – приемник информации». Данная схема подходит для защиты информации как при ее передаче по каналам связи, так и при ее хранении. В последнем случае вместо «канала передачи данных» будет «место хранения данных».

Исследуемая система шифрования с использованием динамического хаоса основана на схеме «хаотический передатчик – хаотический приемник», где взаимодействие передатчика и приемника осуществляется при хаотическом синхронном отклике [8]. Особенностью такой схемы является то, что в ней не требуется внешней синхронизации, т. е. для принимающей стороны не требуется знания начальных условий. Информационный сигнал, поступающий на вход хаотического передатчика, шифруется путем преобразования в хаотический сигнал, который содержит внутри себя информационный сигнал. Далее хаотический сигнал передается на вход хаотического приемника, в котором он преобразуется в исходный информационный сигнал.

Важная роль в процессе построения системы шифрования отводится выбору структуры и параметров хаотического передатчика и приемника. По результатам анализа различных вариантов схем передачи информации на основе синхронного хаотического отклика выберем схему с нелинейным подмешиванием информационного сигнала к хаотическому. Данная схема рассматривается как простой и в то же время эффективный способ защиты информации. Важными особенностями этой схемы по отношению к другим возможным схемам передачи информации на основе динамического хаоса являются: точное извлечение информации из смеси с хаотическим сигналом, самосинхронизация передатчика и приемника, простота аппаратной и программной реализации [8, 17].

Структурная схема рассматриваемой системы шифрования состоит из следующих элементов (рис. 1):

– нелинейного преобразователя (хаотического отображения $F(X)$);

– фильтра (единичной задержки Z^{-1});

– сумматора (вычитателя).

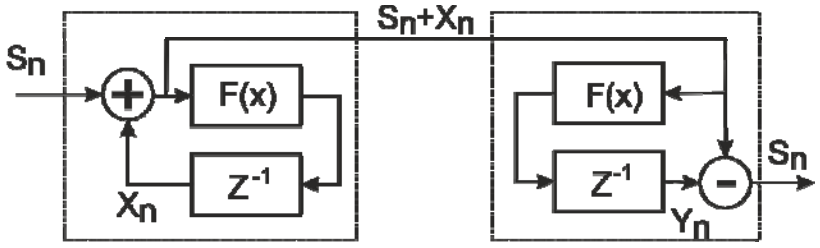

Рис. 1. Структурная схема системы шифрования: S_n – информационный сигнал; X_n – хаотический сигнал, сформировавшийся в передатчике после прохождения нелинейного преобразователя; Y_n – сигнал, прошедший в приемнике цепь обратной связи

В качестве хаотического отображения использовано tent-отображение (рис. 2). Непрерывное отображение $f(x)$ задается уравнением

$$f(x)=\begin{cases}\dfrac{x}{\mu}, & 0 \le x < \mu; \\ \dfrac{1-x}{1-\mu}, & \mu \le x \le 1, \end{cases} \tag{1}$$

где μ – параметр, характеризующий отображение; x и $f(x)$ – действительные числа, принадлежащие промежутку от 0 до 1.

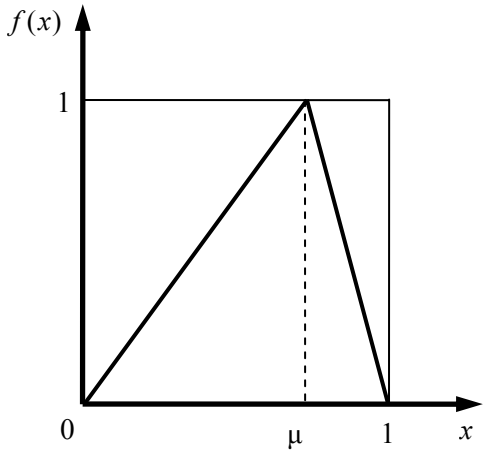

Рис. 2. Внешний вид tent-отображения

Из анализа функции (1) следует, что для данного отображения показатель Ляпунова положителен. Это свидетельствует о том, что хаотическое поведение tent-отображения наблюдается на всем промежутке допустимых значений параметра μ.

Рассмотрим значимость параметра μ. Указанный параметр является главной и единственной характеристикой отображения, определяет свойства и выходные последовательности хаотического отображения, что, в свою очередь, определяет результат процесса шифрования данных с помощью предложенной схемы. Два хаотических tent-отображения с двумя различными параметрами μ определяют две различные системы шифрования, поэтому μ можно рассматривать как параметр, определяющий результат зашифрования, а именно как ключ шифрования.

2. Реализация системы шифрования на практике

Для апробации работы системы на практике, а также для анализа ее крипкостойкости разработано программное обеспечение, которое осуществляет кодирование и декодирование информа-

ции согласно представленной выше схеме. Однако у программной реализации данной схемы имеются определенные и весьма существенные особенности, которые не позволяют реализовать ее в исходном виде. Дело в том, что во всех структурных элементах системы шифрования фигурируют действительные числа. Как известно, представление действительных чисел в памяти компьютера неизбежно сопряжено с появлением погрешностей их представления, причина которых заключается в ограниченности объема памяти для хранения данных. Неточное представление действительных чисел неизбежно ведет к ошибкам в результатах вычислений, что сказывается на поведении «квазинепрерывного» хаотического отображения, а следовательно, ведет к расхождению получаемых результатов с достоверными. В данной ситуации и проявляется принципиальное отличие хаотических систем от криптографических: первые оперируют с действительными числами, в то время как вторые – с целыми. Данное отличие одной системы от другой накладывает принципиальное ограничение применения непрерывных отображений при реализации схемы кодирования с помощью компьютера, поскольку точность представлений действительных чисел в компьютере ограничена объемом доступной памяти. Таким образом, необходим поиск других методов, которые позволят обойти это принципиальное ограничение, а не улучшить точность вычислений.

В качестве одного из таких методов предлагается использовать дискретное (цифровое, целочисленное) отображение вместо непрерывного. Под дискретным отображением здесь понимается отображение, оперирующее целыми числами. Непрерывному tent-отображению $f(x)$ соответствует дискретное tent-отображение $F(x)$, которое задается выражением [18]

$$F(X)=\begin{cases}\left\lceil \dfrac{A}{M}X \right\rceil, & 1\le X<M;\\ \left\lfloor \dfrac{A}{A-M}(A-X) \right\rfloor+1, & M\le X\le A,\end{cases} \tag{2}$$

где $\lfloor a \rfloor$ – наибольшее целое число, не превышающее a, и $\lceil a \rceil$ – наименьшее целое число не ниже чем a; X, $F(X)$ и M – параметры, характеризующие дискретное отображение аналогично параметрам x, $f(x)$, μ для непрерывного отображения.

Поскольку дискретное отображение работает с целыми числами, уже нет необходимости беспокоиться о точности представления данных в памяти компьютера. Переход от теоретических конструкций к практической реализации не вносит упомянутых выше трудностей. Для программной реализации дискретного отображения можно воспользоваться программными библиотеками для работы с числами неограниченной точности. В качестве примера такой библиотеки можно привести работу [19], библиотека которой является наиболее распространенной и производительной на сегодняшний день.

Важным вопросом, подлежащим рассмотрению на этапе программной реализации, является вопрос о величине параметра A. Ее верхняя граница определяется размерностью параметра, т. е. количеством бит, отведенных в памяти компьютера для представления значения данного параметра.

Параметры A и M, а также переменная X имеют одинаковую размерность, с помощью которой определяют количество различных чисел, участвующих в работе отображения. Таким образом, с помощью размерности параметров выбираются размерность и количество возможных значений ключа шифрования, что является одной из основных характеристик любой системы шифрования.

Что касается двух оставшихся структурных элементов схемы в программной реализации, то единичная задержка представляет собой задержку на одну итерацию цикла шифрования, а суммирование, как и вычитание, реализуется операцией побитового сложения по модулю два.

3. Анализ крипкостойкости

Проведем анализ криптостойкости схемы шифрования с дискретным tent-отображением. Анализ криптостойкости представляет собой достаточно трудоемкий процесс. Выделяют сле-

дующие направления исследования криптостойкости алгоритмов шифрования: теоретическую криптостойкость, практическую криптостойкость, имитостойкость [14]. Одним из направлений исследования теоретической криптостойкости является стойкость к статистическим атакам, одним из вариантов которых является частотный криптоанализ. Практическая криптостойкость определяет стойкость алгоритма шифрования к различным видам криптоатак: на основе известного открытого текста, выбранного открытого текста, выбранного шифртекста, адаптированного открытого или шифртекста. Последние из указанных являются наиболее благоприятными для нападающего. К одним из видов криптоаналитических атак на основе выбранных или адаптированных текстов относят дифференциальный (разностный) криптоанализ и линейный криптоанализ, а также производные от них методы [15].

В рассматриваемой работе проанализирована криптостойкость представленной системы шифрования с позиций частотного криптоанализа и стойкости к атаке методом грубой силы.

3.1. Частотный криптоанализ

Суть частотного криптоанализа состоит в получении спектральной характеристики текста путем подсчета частоты, с которой каждый символ алфавита встречается в тексте. В спектре открытого текста отчетливо проявляются закономерности и особенности, характерные для данного алфавита и типа открытого текста. Например, в русском языке буквы «а», «о», «е» встречаются чаще, чем буквы «э», «ю», «я».

Для экспериментов в качестве открытого текста выбран фрагмент текста на русском языке, который является характерным для данного языка текстом, выбранным случайным образом. Объем выборки составляет 11 КБ. Результаты частотного криптоанализа приведены на рис. 3 и 4. На каждом из рисунков по оси X отложен код символа (C), по оси Y – количество повторений данного символа в тексте (N).

Сравнивая спектры открытого и шифртекстов, можно судить о надежности сокрытия информации системой шифрования и о вероятности успешного проведения злоумышленником частотного криптоанализа [15].

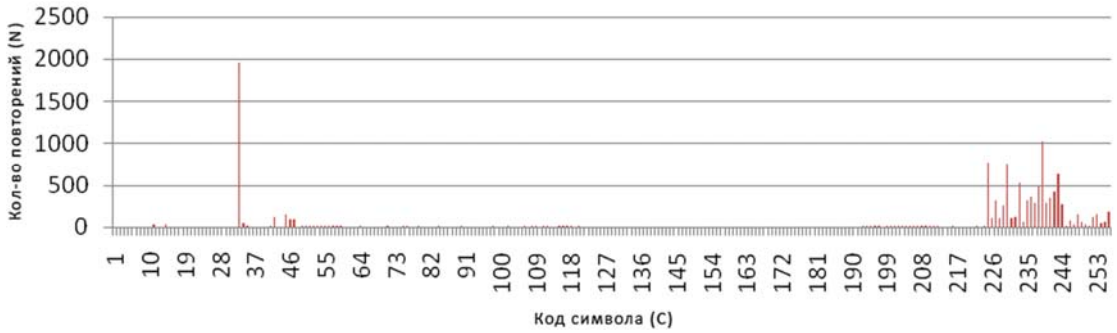

Рис. 3. Результаты частотного анализа открытого текста

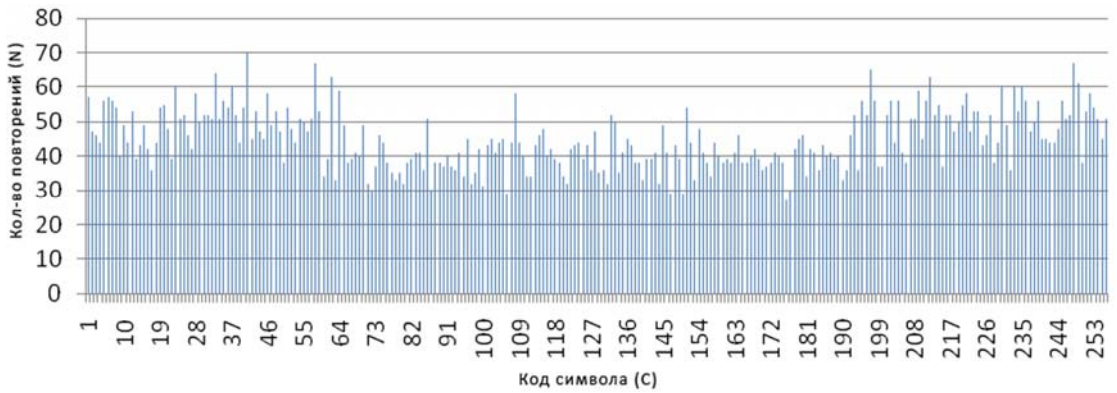

Рис. 4. Результаты частотного анализа шифртекста,
полученного с помощью предложенной системы шифрования

Для количественной оценки надежности сокрытия информации введем коэффициент надежности сокрытия информации k, характеризующий степень корреляции спектра шифртекста с равномерным спектром для данного объема информации:

$$k = \frac{K}{K_{\max}}, \tag{3}$$

где K – степень корреляции (скалярное произведение) спектра шифртекста с равномерным спектром; $K_{\max}$ – степень корреляции спектра открытого текста с равномерным спектром.

Было установлено, что в спектре шифртекста отсутствуют компоненты открытого текста при значениях параметра $k \le 0,003$. После определения количественной оценки надежности сокрытия информации, а также порогового значения для соответствующего коэффициента k был проведен расчет данного коэффициента для различных значений параметра M дискретного tent-отображения (табл. 1). Размерность параметра M выбрана равной 64 битам (8 байтам).

Таблица 1

Коэффициенты степени корреляции для различных значений параметра M

Ключ M	Коэффициент надежности сокрытия информации k
0x0000000000000001	0,002949
0x1111111111111111	0,001559
0x2222222222222221	0,001505
0x3333333333333331	0,001682
0x4444444444444441	0,001622
0x5555555555555551	0,001573
0x6666666666666661	0,001204
0x7777777777777771	0,00142
0x8888888888888881	0,00136
0x9999999999999991	0,001561
0xAAAAAAAAAAAAAAA1	0,001239
0xBBBBBBBBBBBBBBB1	0,001507
0xCCCCCCCCCCCCCCC1	0,001427
0xDDDDDDDDDDDDDDD1	0,001811
0xEEEEEEEEEEEEEEE1	0,001717
0xFFFFFFFFFFFFFFFF	0,001946

Ключи (значения параметра M) были равномерно выбраны на интервале (0x0000000000000001 – 0xFFFFFFFFFFFFFFFF). Из табл. 1 видно, что ни одно из значений параметра k не превысило установленное пороговое значение в 0,003. Учитывая полученные данные, можно сделать вывод о том, что на всем интервале ключей схема шифрования является стойкой по отношению к частотному криптоанализу.

3.2. Атака методом грубой силы

Суть атаки методом грубой силы состоит в полном переборе всех значений ключа шифрования и выявлении исходного ключа, с помощью которого производилось зашифрование. Это достаточно простой и универсальный (применимый к любым системам шифрования) способ взлома системы шифрования и в то же время наиболее ресурсоемкий (в плане вычислительных ресурсов и времени). Тем не менее это первый вид атак, стойкость к которому необходимо исследовать, разрабатывая новый шифр. Кроме того, вычислительные ресурсы в последнее время стремительно растут, поэтому данным видом атаки не стоит пренебрегать.

В результате исследования стойкости предложенной системы шифрования к данному виду атак было установлено, что расшифрование зашифрованного текста будет успешным

или почти успешным даже в том случае, когда ключ, используемый для расшифрования, не совпадает с ключом, используемым для зашифрования. Чем ближе подбираемый ключ к исходному, тем «четче» получаемый на выходе результат расшифрования. Поэтому основная задача – определить, в зависимости от параметров схемы шифрования, насколько сильно должен отличаться подобранный ключ от исходного, чтобы результат расшифрования таким ключом был успешным.

Для решения поставленной задачи предложена следующая методика. Сначала определяется область в формируемом ключе (область R), при наличии ошибок в которой получаем близкий к исходному результат расшифрования. Размер этой области определяется в битах и является величиной, характеризующей стойкость конкретной системы шифрования с определенными параметрами к атаке методом грубой силы. Данный параметр позволяет оценить степень сходства подбираемого и исходного ключей. Соответственно чем меньше размер области R, тем более близкий к исходному ключ необходимо подобрать для успешного расшифрования. Для системы шифрования, стойкой к полному перебору ключей, размер этой области должен быть равен нулю.

Определение размера области R проводилось по следующей схеме. Выбирался ключ M, с помощью которого открытый текст зашифровывался. Затем методом двоичного поиска производился поиск такого ключа из всего промежутка, для которого коэффициент степени корреляции k расшифрованного текста равнялся пороговому значению 0,003. Данный метод может быть применен, так как коэффициент степени корреляции k расшифрованного текста тем ближе к единице, чем выбранный из всего исследуемого интервала ключ ближе к исходному ключу шифрования. Далее проводилось сравнение полученного таким образом порогового ключа с исходным ключом. Количество бит, в которых данные ключи различаются (в которых можно сделать ошибку), и принималось за значение размера области R. Соответственно, для того чтобы система была стойкой к атаке методом грубой силы, размер области R для каждого ключа должен быть равен нулю.

Из табл. 2 видно, что размер области R почти равен размерности самого ключа шифрования (64 бит). Можно сделать вывод, что представленная система шифрования совершенно не является стойкой к атаке методом грубой силы. Поэтому отсутствует необходимость рассматривать другие виды атак.

Таблица 2

Размеры области R для различных значений ключа (параметра M хаотического отображения)

Ключ M	Размер области R, бит
0x0000000000000001	62
0x1111111111111111	62
0x2222222222222221	62
0x3333333333333331	62
0x4444444444444441	61
0x5555555555555551	61
0x6666666666666661	61
0x7777777777777771	61
0x8888888888888881	61
0x9999999999999991	61
0xAAAAAAAAAAAAAAA1	61
0xBBBBBBBBBBBBBBB1	61
0xCCCCCCCCCCCCCCC1	61
0xDDDDDDDDDDDDDDD1	62
0xEEEEEEEEEEEEEEE1	62
0xFFFFFFFFFFFFFFFF	62

4. Модификация схемы и ее криптоанализ

Для обеспечения устойчивости схемы к атаке методом грубой силы предлагается ее модификация (рис. 5). Единичное применение хаотического отображения на каждой итерации цикла шифрования заменим последовательностью из n применений.

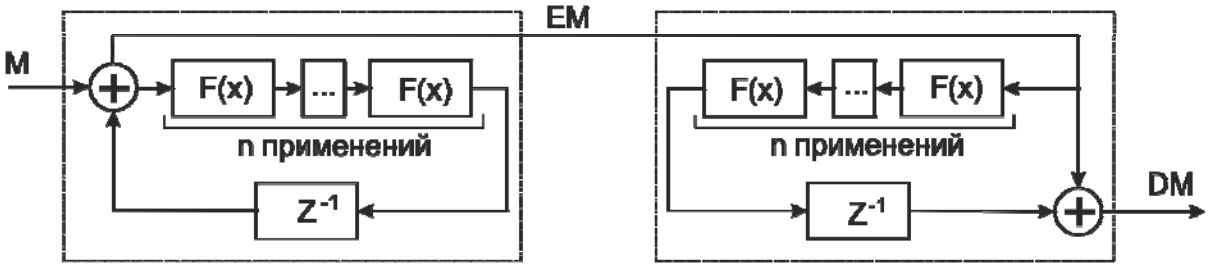

Рис. 5. Модифицированная схема шифрования:
EM – зашифрованное сообщение; DM – расшифрованное сообщение

Проведем криптоанализ модифицированной схемы шифрования методами, описанными в разд. 3. В ячейках табл. 3 – значения коэффициентов надежности сокрытия информации k, серым выделены те ячейки, значения в которых превосходят установленное пороговое значение коэффициента k величиной 0,003.

Таблица 3

Результаты статистического криптоанализа в зависимости
от ключа шифрования M и количества применений хаотического отображения n

Ключ M	Количество применений хаотического отображения n								
	1	10	20	30	40	50	60	70	80
0x0000000000000001	0,0029	0,0472	0,0648	0,0494	0,0020	0,0065	0,0516	0,0305	0,0017
0x1111111111111111	0,0015	0,0015	0,0013	0,0014	0,0015	0,0017	0,0016	0,0013	0,0014
0x2222222222222221	0,0015	0,0015	0,0016	0,0015	0,0015	0,0014	0,0016	0,0016	0,0014
0x3333333333333331	0,0016	0,0016	0,0016	0,0017	0,0014	0,0013	0,0013	0,0016	0,0014
0x4444444444444441	0,0016	0,0016	0,0015	0,0015	0,0013	0,0014	0,0015	0,0015	0,0014
0x5555555555555551	0,0015	0,0013	0,0015	0,0015	0,0016	0,0014	0,0013	0,0014	0,0015
0x6666666666666661	0,0012	0,0014	0,0016	0,0014	0,0016	0,0014	0,0014	0,0015	0,0014
0x7777777777777771	0,0014	0,0013	0,0015	0,0015	0,0014	0,0014	0,0016	0,0016	0,0012
0x8888888888888881	0,0013	0,0016	0,0012	0,0015	0,0015	0,0016	0,0015	0,0012	0,0014
0x9999999999999991	0,0015	0,0015	0,0016	0,0013	0,0015	0,0016	0,0015	0,0015	0,0012
0xAAAAAAAAAAAAAAA1	0,0012	0,0015	0,0013	0,0014	0,0012	0,0016	0,0018	0,0014	0,0014
0xBBBBBBBBBBBBBBB1	0,0015	0,0015	0,0014	0,0013	0,0015	0,0016	0,0015	0,0012	0,0014
0xCCCCCCCCCCCCCCC1	0,0014	0,0016	0,0014	0,0011	0,0016	0,0013	0,0016	0,0013	0,0015
0xDDDDDDDDDDDDDDD1	0,0018	0,0014	0,0018	0,0013	0,0014	0,0011	0,0016	0,0016	0,0014
0xEEEEEEEEEEEEEEE1	0,0017	0,0015	0,0014	0,0014	0,0013	0,0016	0,0013	0,0016	0,0014
0xFFFFFFFFFFFFFFFF	0,0019	0,0017	0,0102	0,0043	0,0016	0,0103	0,0101	0,0029	0,0023

Результаты вычислений размера области R в зависимости от ключа шифрования M и количества применений n хаотического отображения представлены в табл. 4, в ячейках – значения размера области R.

Из табл. 4 видно, что в пространстве ключей M при количестве применений отображения n появляются области с нулевым размером области R. Значит, для успешного расшифро-

вания сообщения следует использовать именно исходный ключ, что свидетельствует о стойкости системы к атаке методом грубой силы в определенном интервале значений ключа.

Таблица 4

Результаты анализа шифра на устойчивость к атаке методом грубой силы

Номер N	Ключ M	Количество применений хаотического отображения n								
		1	10	20	30	40	50	60	70	80
1	0x0000000000000001	62	59	58	57	57	56	56	56	56
2	0x1111111111111111	62	57	53	50	47	44	40	38	35
3	0x2222222222222221	62	55	50	45	39	34	29	23	18
4	0x3333333333333331	62	54	47	40	33	26	19	12	6
5	0x4444444444444441	61	53	45	36	28	21	12	4	0
6	0x5555555555555551	61	53	44	34	25	16	7	0	0
7	0x6666666666666661	61	52	42	33	23	13	4	0	0
8	0x7777777777777771	61	52	42	32	22	12	3	0	0
9	0x8888888888888881	61	52	42	32	22	12	3	0	0
10	0x9999999999999991	61	52	42	33	22	13	4	0	0
11	0xAAAAAAAAAAAAAAA1	61	52	43	34	25	15	7	0	0
12	0xBBBBBBBBBBBBBBB1	61	53	45	36	28	20	11	4	0
13	0xCCCCCCCCCCCCCCC1	61	54	46	40	33	25	19	12	5
14	0xDDDDDDDDDDDDDDD1	62	54	49	44	39	34	28	23	18
15	0xEEEEEEEEEEEEEEE1	62	56	53	49	46	43	39	37	34
16	0xFFFFFFFFFFFFFFFF	62	59	58	57	57	57	56	56	56

Подобные исследования были проведены также для размерностей ключа шифрования 16 бит, 32 бита (рис. 6).

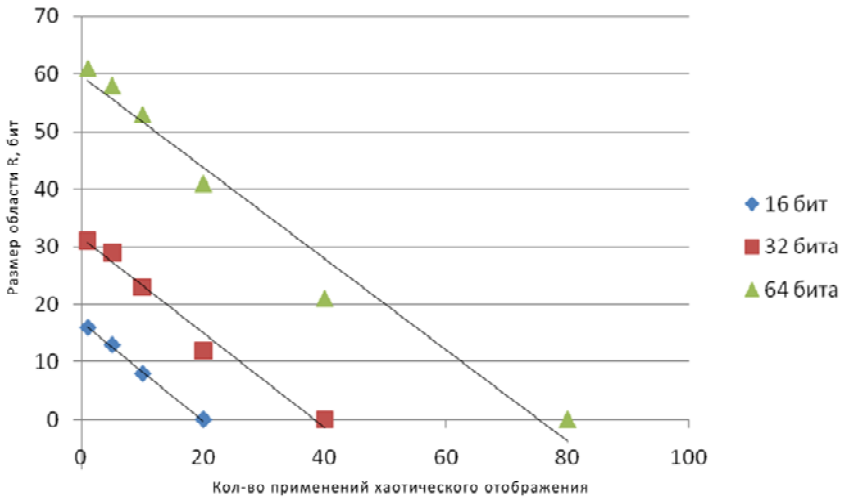

Рис. 6. Экспериментальные графики зависимости размера области R от количества применений хаотического отображения n для разных размерностей ключа шифрования

Результаты показывают, что для любого размера ключа имеется такое количество итераций хаотического отображения n, при котором данная схема оказывается стойкой к атаке методом грубой силы. Предельное значение количества итераций отображения определяется значением точки на оси абсцисс, в которой прямая аппроксимации пересекает данную ось.

5. Сравнение с другими известными видами отображений

Проведем сравнение результатов работы схемы шифрования с tent-отображением и схемы с полиномиальными отображениями Чебышева, которые задаются рекурсивным выражением

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \quad (4)$$

где $n \geq 2$ – степень отображения и соответствующего ему полинома; $T_0(x) = 1$ и $T_1(x) = x$.

Хорошо известно, что при $n \geq 2$ отображение (4) обладает хаотическими свойствами, а показатель Ляпунова положителен [18]. Соответствующее дискретное отображение имеет вид

$$F(X) = T_n(X) \bmod M, \quad (5)$$

где X, M – целые числа; оператор mod означает остаток от деления.

Зашифруем тот же самый фрагмент открытого текста шифром, в котором в качестве нелинейного преобразователя F выступает дискретное отображение Чебышева. На графике спектрального анализа полученного шифртекста (рис. 7) по оси X отложен код символа (C), по оси Y – количество повторений данного символа в тексте (N).

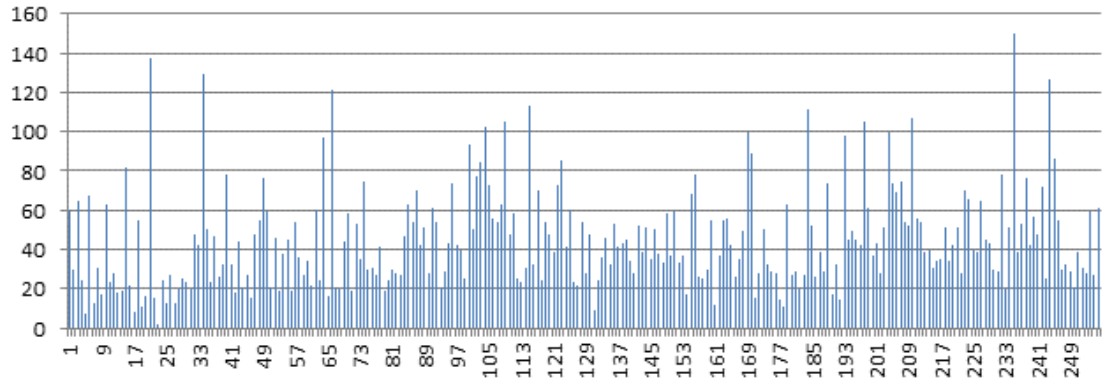

Рис. 7. Результаты частотного анализа шифртекста, полученного с помощью исследуемой системы шифрования и отображения Чебышева

При сравнении спектров открытого текста (см. рис. 3) и шифртекста (рис. 7) установлено, что применение в схеме шифрования отображения Чебышева наравне с tent-отображением позволяет надежно скрывать факт наличия передаваемой информации в сигнале, а также сводит вероятность успешного проведения злоумышленником частотного криптоанализа к минимуму.

Для системы шифрования на основе отображения Чебышева исследованы элементы стойкости к атаке методом грубой силы. При этом проведено расшифрование шифртекста ключом, соседним к использованному при зашифровании. В данном случае термин «соседний ключ» обозначает следующий по порядку ключ в множестве всех ключей. Спектральный анализ (рис. 8) полученного в результате такого расшифрования текста показал, что, в отличие от tent-отображения, в тексте не просматриваются структуры открытого текста. На рис. 8 по оси X отложен код символа C, по оси Y – количество повторений N данного символа в тексте.

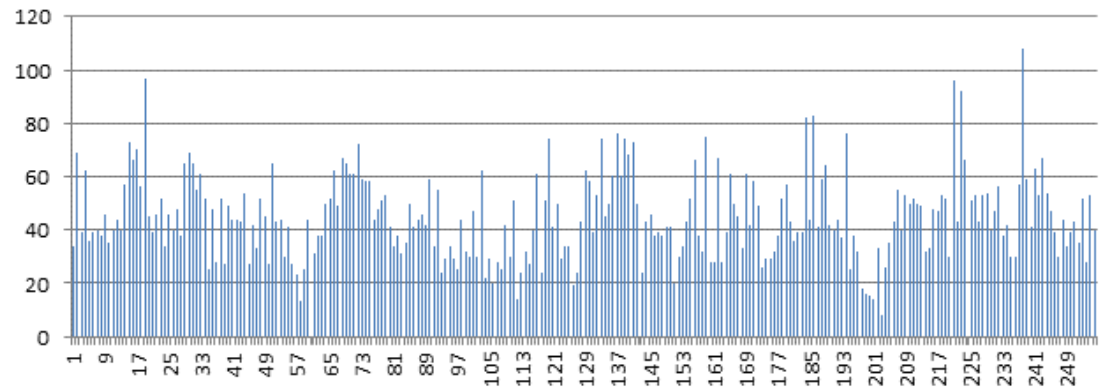

Рис. 8. Результаты частотного анализа текста, полученного при попытке расшифровать зашифрованный текст соседним ключом

Результаты, полученные при использовании в схеме шифрования отображения Чебышева, свидетельствуют о необходимости дальнейших исследований.

Заключение

В работе рассмотрены вопросы, связанные с применением методов хаотической динамики для решения криптографических задач. Основным компонентом схемы шифрования на основе динамического хаоса является хаотическое отображение, выбор которого определяет криптостойкость схемы шифрования. В качестве хаотического отображения в предложенной схеме выбрано дискретное tent-отображение. Анализ криптостойкости схемы шифрования включает в себя статистический криптоанализ, а также анализ на устойчивость к атаке методом грубой силы. Совмещение результатов анализа криптостойкости позволило выявить условия, при которых система шифрования является стойкой как к частотному криптоанализу, так и к атаке методом грубой силы.

Список литературы

1. Виланский, Ю.В. Двухканальный алгоритм шифрования MV2 / Ю.В. Виланский, В.В. Лепин, В.А. Мищенко // Вести Института современных знаний. – 2003. – № 3.– С. 113–121.

2. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М. : Гелиос АРВ, 2006. – 376 с.

3. Демьянович, Ю.К. Вейвлетные разложения и шифрование / Ю.К. Демьянович, А.Б. Левина // Методы вычислений. – СПб. : Изд-во С.-Петерб. ун-та, 2008. – Вып. 22. – С. 41–63.

4. Шниперов, А.Н. Синтез и анализ высокоскоростных симметричных криптосистем на основе управляемых операций / А.Н. Шниперов // Информационные технологии. – М. : Новые технологии, 2008. – № 1. – С. 36–41.

5. Вавренюк, В.Г. Симметричная схема шифрования на основе помехоустойчивого каскадного кода / В.Г. Вавренюк, П.Н. Корнюшин // Системная интеграция и безопасность ; под ред. А.А. Шелупанова. – Томск : Институт оптики атмосферы СО РАН, 2006. – Вып. 1. – С. 116–118.

6. Кшевецкий, А.С. Уменьшение размера открытого ключа в криптосистемах на линейных ранговых кодах / А.С. Кшевецкий // Безопасность информационных технологий (БИТ). – 2006. – № 1. – С. 1–8.

7. Плонковски, М. Использование нейронных сетей в системах криптографического преобразования информации / М. Плонковски, П. Урбанович // Известия Белорусской инженерной академии. – 2004. – № 1(17)/4. – С. 13–15.

8. Дмитриев, А.С. Динамический хаос. Новые носители информации для систем связи / А.С. Дмитриев, А.И. Панас. – М. : Физматлит, 2002. – 205 с.

9. Сидоренко, А.В. Информационные аспекты нелинейной динамики / А.В. Сидоренко. – Минск : БГУ, 2008. – 125 с.

10. Птицын, Н. Приложение теории детерминированного хаоса в криптографии / Н. Птицын. – М., 2002. – 150 с.

11. Дмитриев, А.А. Хаотические последовательности, содержащие заданную информацию / А.А. Дмитриев // Радиотехника и электроника. – 2002. – Т. 47, № 11. – С. 1370–1375.

12. Nonlinear-dynamic systems of confidential communication: classification, simulation, experiment / I. Izmailov [et al.] // ENOC 2008. – Saint Petersburg, 2008. – P. 1–6.

13. Experimental demonstration of secure communications via chaotic synchronization / L. Kocarev [et al.] // Int. J. Bifurcation and Chaos. – 1992. – № 3. – P. 709–713.

14. Молдавян, Н.А. Введение в криптосистемы с открытым ключом / Н.А. Молдавян, А.А. Молдавян. – СПб. : БХВ-Петербург, 2005. – 288 с.

15. Основы криптографии / А.П. Алферов [и др.]. – М. : Гелиос АРВ, 2005. – 480 с.

16. Анищенко, В.С. Нелинейная динамика хаотических и стохастических систем / В.С. Анищенко, Т.Е. Вадивасова, В.В. Астахов. – Саратов : Изд-во Саратовского университета, 1999. – 368 с.

17. Сидоренко, А.В. Анализ криптостойкости систем шифрования на основе динамического хаоса / А.В. Сидоренко, К.С. Мулярчик // Информационные системы и технологии : тр. Междунар. конф. IST'2009. – Минск : БГУ, 2009. – С. 75–76.

18. Amigo, J.M. Theory and practice of chaotic cryptography / J.M. Amigo, L. Kosarev, J. Szczepanski // Phys. Lett. A. – 2007. – Vol. 366. – P. 211–216.

19. The GNU Multiple Precision Arithmetic Library [Electronic recourse]. – Mode of access : http://gmplib.org. – Date of access : 02.03.2010.

Поступила 10.03.10

Белорусский государственный университет,
Минск, пр. Независимости, 4
e-mail: sidorenkoA@bsu.by

A.V. Sidorenko, K.S. Mulyarchik

A MODIFICATION OF THE METHOD OF DATA ENCRYPTION BASED ON THE DYNAMIC CHAOS

A method of information security and practical implementation of the encryption system based on the self-synchronization phenomena in dynamic chaos systems that is also called synchronous chaotic reply effect are considered. It is suggested to use the discrete tent-mapping as the key element of the coding scheme. The security analysis of the encryption system to statistical and brute-force attacks is described. A modification of the encryption system allowed improving the robustness against all kinds of statistical and brute-force attacks.